

This listing of claims will replace all prior versions, and listings, of claims in the application

LISTING OF CLAIMS

1-14. (cancelled).

15. (new) An invalidity-monitoring program for monitoring invalid data which causes a computer to execute an invalid operation, comprising:

software that acquires input/output data that is input or output over a network that is connected to said computer, or over an externally connected bus that connects said computer with an external device;

software that identifies ID information from said input/output data for identifying a user;

software that acquires at least part of attribute data corresponding to said ID information from a user-information-storage unit that stores attribute information for all users having authorization to use said computer;

software that references a determination-rule-storage unit that stores rules for determining whether said input/output data is invalid data, and determines whether said input/output data is invalid data; and

software that stops execution by said input/output data when it is determined in said invalid-data-determination that said input/output data is invalid data;

wherein

said determination-rule-storage unit stores determination rules that correspond to user attributes; and

software that references, in said determining of whether said input/output data is invalid data, said determination rules that correspond to attribute information acquired in the acquisition of attribute information determines whether said input/output data is invalid.

16. (new) The invalidity-monitoring program of claim 15, further comprising:

software that references said user-information-storage unit and determines whether the user corresponding to said ID information has authorization to use said computer; and

software that stops operation by said input/output data when it is determined in the determination of authorization that there is no authorization to use said computer;

wherein

said software that determines authorization performs this before it is determined whether said input/output data is invalid data, and when it is determined in the determining authorization that there is no authorization to use said computer, said program causes said computer to not execute at least one of the following: acquiring attribute information and said determination of whether said input/output data is invalid data.

17. (new) The invalidity-monitoring program of claim 15, further comprising:

software that references a profile-storage unit that stores log data related to said input/output data as profiles for each user, and compares input/output data that was acquired in said data-acquisition with a

normal operation trend of said user to determine whether operation is unusual; and

software that stops an operation executed by said input/output data in said stopping operation executed by said input/output data also when it is determined in said determining whether operation is unusual that that operation is unusual.

18. (new) The invalidity-monitoring program of claim 15, further comprising software that executes a process of interrupting a session in said stopping of the operation executed by said input/output data when said input/output data is acquired from a network in said acquisition of input/output data.

19. (new) The invalidity-monitoring program of claim 15, further comprising software that stops the process of executing a driver in the stopping of the operation executed by said input/output data when said input/output data is acquired from an externally connected bus in said acquisition of input/output data.

20. (new) An invalidity-monitoring program for monitoring invalid data which causes a computer to execute an invalid operation, comprising:

software that acquires input/output data that is input or output over a network that is connected to said computer, or over an externally connected bus that connects said computer with an external device;

software that identifies ID information from said input/output data for identifying a user;

software that acquires at least part of attribute data corresponding to said ID information from a user-information-storage unit that stores attribute information for all users having authorization to use said computer;

software that references a determination-rule-storage unit that stores rules for determining whether said input/output data is invalid data, and determining whether said input/output data is invalid data; and

software that notifies a terminal being operated by said user or administrator that an operation being executed by said input/output data is an invalid operation when it is determined in said determining whether said input/output data is invalid that said input/output data is invalid data;

wherein

said determination-rule-storage unit stores determination rules that correspond to user attributes; and

software that references, in said step of determining whether said input/output data is invalid data, said determination rules that correspond to attribute information acquired in said step of acquiring attribute information to determine whether said input/output data is invalid data.

21. (new) An invalidity-monitoring method for monitoring invalid data, which causes a computer to execute an invalid operation, comprising:

acquiring, by said computer, input/output data that is input or output over a network that is connected to said computer, or over an externally connected bus that connects said computer with an external device;

identifying, by said computer, ID information from said input/output data for identifying a user;

acquiring, by said computer, at least part of attribute data corresponding to said ID information from a user-information-storage unit that stores attribute information for all users having authorization to use said computer;

referencing, by said computer, a determination-rule-storage unit that stores rules for determining whether said input/output data is invalid data;

determining whether said input/output data is invalid data based on said rules; and

stopping, by said computer, execution by said input/output data when it is determined in said invalid-data-determination step that said input/output data is invalid data;

wherein

said determination-rule-storage unit stores determination rules that correspond to user attributes; and

in said step of determining whether said input/output data is invalid data, referencing said determination rules that correspond to attribute information acquired in said step of acquiring attribute information to determine whether said input/output data is invalid.

22. (new) An invalidity-monitoring method for monitoring invalid data, which causes a computer to execute an invalid operation, comprising:

acquiring, by said computer, input/output data that is input or output over a network that is connected to said computer, or over an externally

connected bus that connects said computer with an external device;

identifying, by said computer, ID information from said input/output data for identifying a user;

acquiring, by said computer, at least part of attribute data corresponding to said ID information from a user-information-storage unit that stores attribute information for all users having authorization to use said computer;

referencing, by said computer, a determination-rule-storage unit that stores rules for determining whether said input/output data is invalid data;

determining whether said input/output data is invalid data; and

notifying, by said computer, a terminal being operated by said user or administrator that an operation being executed by said input/output data is an invalid operation when it is determined in said step of determining whether said input/output data is invalid that said input/output data is invalid data;

wherein

said determination-rule-storage unit stores determination rules that correspond to user attributes; and

in said step of determining whether said input/output data is invalid data, referencing said determination rules that correspond to attribute information acquired in said step of acquiring attribute information to determine whether said input/output data is invalid.

23. (new) An invalidity-monitoring system for monitoring invalid data, which causes a computer to execute an invalid operation, the system comprising:

a computer having a connection to a network or to an external device;

a data-acquisition mechanism for acquiring input/output data that is input or output over the network that is connected to said computer, or over an externally connected bus that connects said computer with the external device;

an ID-information-identifier for identifying ID information from said input/output data for identifying a user;

a user-information-store for storing attribute information for all users having authorization to use said computer;

an attribute-information acquisition mechanism for acquiring at least part of the attribute data corresponding to said ID information from said user-information-store;

a determination-rule-store for storing rules for determining whether said input/output data is invalid data;

an invalid-data-determination mechanism for referencing said determination-rule-store, and determining whether said input/output data is invalid data; and

a stoppage mechanism for stopping execution by said input/output data when it is determined by said invalid-data-determination mechanism that said input/output data is invalid data;

wherein

said determination-rule-store stores determination rules that correspond to user attributes; and

said invalid-data-determination mechanism references said determination rules that correspond to attribute information acquired by said attribute-information-acquisition mechanism to determine whether said input/output data is invalid.

24. (new) The invalidity-monitoring system of claim 23 further comprising:
a use-authorization-determination mechanism for referencing said user-
information-store and determining whether the user corresponding
to said ID information has authorization to use said computer;

wherein

said stoppage mechanism also stops operation executed by said
input/output data when it is determined by said use-authorization-
determination mechanism that there is no authorization to use said
computer;

said use-authorization-determination mechanism is activated before said
invalid-data-determination mechanism; and

when it is determined by said use-authorization-determination mechanism
that there is no authorization to use said computer, at least one of
the following; said attribute-information-acquisition mechanism or
said invalid-data-determination mechanism does not execute.

25. (new) The invalidity-monitoring system of claim 23 further comprising:
a profile-store for storing log data related to said input/output data as
profiles for each user; and

an unusual-operation-determination mechanism for referencing said
profile-store and comparing input/output data that was acquired by
said data-acquisition mechanism with the normal operation trend of
said user to determine whether operation is unusual;

wherein

said stoppage mechanism also stops an operation executed by said input/output data when it is determined by said unusual-operation-determination mechanism that operation is unusual.

26. (new) The invalidity-monitoring system of claim 23, wherein said stoppage mechanism executes a process of interrupting a session when said data-acquisition mechanism acquired said input/output data from a network.

27. (new) The invalidity-monitoring system of claim 23, wherein said stoppage mechanism stops a process of executing a driver when said data-acquisition mechanism acquired said input/output data from an externally connected bus.

28. (new) An invalidity-monitoring system for monitoring invalid data, which causes a computer to execute an invalid operation, the system comprising:

- a computer having a connection to a network or to an external device;
- a data-acquisition mechanism for acquiring input/output data that is input or output over the network that is connected to said computer, or over an externally connected bus that connects said computer with the external device;
- an ID-information-identification mechanism for identifying ID information from said input/output data for identifying a user;
- a user-information-store for storing attribute information for all users having authorization to use said computer;
- an attribute-information acquisition mechanism for acquiring at least part of the attribute data corresponding to said ID information from said user-information-store;

a determination-rule-storage mechanism for storing rules for determining whether said input/output data is invalid data;

an invalid-data-determination mechanism for referencing said determination-rule-store, and determining whether said input/output data is invalid data; and

a notification mechanism for notifying the terminal being operated by said user or administrator that an operation being executed by said input/output data is an invalid operation when it is determined by said invalid-data-determination means that said input/output data is invalid data;

wherein

said determination-rule-storage mechanism stores determination rules that correspond to user attributes; and

said invalid-data-determination mechanism references said determination rules that correspond to attribute information acquired by said attribute-information-acquisition mechanism to determine whether said input/output data is invalid.